Dependable Wireless Sensor Networks for Prognostics and Health Management: A Survey

W. Elghazel[1], J.M. Bahi[2], C. Guyeux[2], M. Hakem[2], K. Medjaher[1], and N. Zerhouni[1]

[1] *Automatic Control and Micro-Mechatronic Systems Department, FEMTO-ST Institute*
Université de Franche-Comté, Besançon, France
wiem.elghazel@femto-st.fr
kamal.medjaher@ens2m.fr
noureddine.zerhouni@ens2m.fr

[2] *Computer Science and Complex Systems Department, FEMTO-ST Institute*
Université de Franche-Comté, Besançon, France
jacques.bahi@univ-fcomte.fr
christophe.guyeux@univ-fcomte.fr
mhakem@femto-st.fr

ABSTRACT

Maintenance is an important activity in industry as it reduces costs and enhances availability. This can be done either to revive a system/component or to prevent it from breaking down. The increasing need for reliability has led maintenance strategies to evolve from corrective to condition-based and predictive maintenance. The key process of the latter is prognostics and health management, a tool that predicts the remaining useful life of engineering assets. As plants are requested to offer both safety and reliability, planning a maintenance activity requires accurate information about the system/component health state. Usually, this information is gathered through independent sensors or a wired network of sensors. The use of a wireless sensor network has many advantages. First of all, the absence of wires gives sensor networks the ability to cover a large scale surveillance area. Second, it has become possible to monitor hostile and inaccessible areas by simply dropping the sensors from an aircraft to the monitoring region. Finally, the accuracy of measurements can be improved as the sensors can be placed at specific locations without being wired. Even though the deployment of wireless sensor networks is gaining great importance in monitoring applications, there are some research issues that still need to be studied to provide more accurate and reliable data. Indeed, we strongly believe that a good prognostic process starts with a reliable source of information; the wireless sensor network in our case. For this matter, in this paper, we discuss the dependability of wireless sensor networks, we highlight the attributes that have an impact on data accuracy, and present the state of the art in prognostics.

1. INTRODUCTION

Industrial systems are subject to failures, which can be irreversible or result in consequences varying from minor to severe. From this context, it is important to monitor a system, assess its health, and plan maintenance activities to avoid "catastrophic" failure results.

The research in Prognostic and Health Management (PHM) field has led to the development of prognostic models in an attempt to predict the Remaining Useful Life (RUL) of machinery before failure takes place. A maintenance schedule is then decided and system shutdown is prevented. Yet, if the prediction model and the provided measurements are not accurate, it is possible that the maintenance activity will be performed either too soon or too late.

Such a prediction activity requires online measurements of the operating conditions of the system under consideration. This information is usually gathered by the means of sensor nodes. In this study, we consider the case where the nodes communicate their information within a Wireless Sensor Network (WSN). Nevertheless, a WSN is prone to failure due to the nature of communication in the network and to the characteristics of its devices. For this reason, before deployment, a prior dependability study of the network is needed. It is the only way to guarantee the reception of accurate data.

Although both dependability of WSNs and prognostic models development have been studied and reported in the literature, as far as we know, none of the existing research work has

considered the dependability of WSNs for PHM purposes. In real life applications, the provided data can be inaccurate and incomplete. If this is not taken into consideration while building the prognostic model, the provided results cannot be reliable. Considering the limited computational capacities of WSNs, it is very common to privilege some dependability issues over others, regarding the target applications requirements. Thus, it is crucial to consider a "prognostic-oriented" dependability solution for WSNs.

This paper presents dependability issues with WSNs, that are relevant for RUL prediction, and discusses different prognostic approaches. The remainder of the paper is structured as follows. Section 2 presents an overview of wireless sensor networks. A state of the art in prognostics and health management is provided in Section 3. The relation between prognostics and WSN dependability and the remaining challenges are illustrated in Section 4. Finally, a conclusion is given in Section 5.

2. OVERVIEW OF WIRELESS SENSOR NETWORKS

WSNs are event-based systems that rely on the collective effort of several microsensor nodes (Akan & Akyildiz, 2005). This offers the network greater accuracy, larger coverage area, and the possibility to extract localized features. Typically, a WSN is composed of few base stations and hundreds (or thousands) of sensor nodes. A sensor node is a tiny device having the capability of sensing new events, computing the sensed values, and communicating information. Thus, the network can be deployed to monitor physical and environmental phenomena such as temperature, vibrations, light, humidity, etc.

There are different settings for a WSN model, which is generally dynamic, as radio range and network connectivity evolve over time. A network model can be either hierarchical, distributed, centralized, heterogeneous, or homogeneous (Z. Li & Gong, 2011).

2.1. Shortcomings of a WSN

WSNs are designed for an efficient event detection. They consist of a large number of sensor nodes deployed in a surveillance area to detect the occurrence of possible events. Such an activity necessitates efficiency, which is hard to achieve with the constraints of WSNs.

Available energy is a big limitation to WSN capabilities. In fact, sensor nodes are small sized devices, resulting in tiny and non-refillable batteries as energy supply (Carman, Kuus, & Matt, 2000). Moreover, wireless networks are vulnerable and necessitate security codes. Yet, processing security functions, transmitting security related data, and securing storage necessitate extra power, which is critical for WSNs (Carman et al., 2000; Walters, Liang, Shi, & Chaudhary, 2007).

The wireless communication between sensor nodes renders packet loss highly probable. The absence of physical connections in the network can result in channel errors, missing links, and network congestion and cause packet drops. In addition to this, multi-hop routing and node processing lead to great latency and transmission errors in the network.

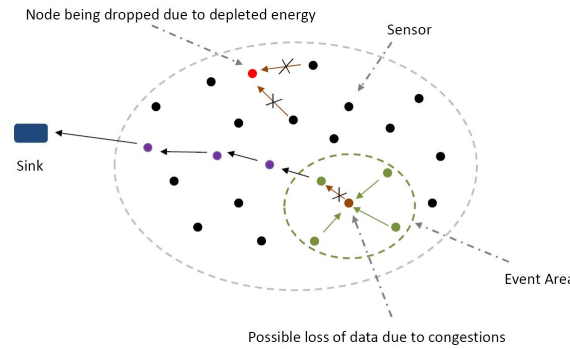

Figure 1. Illustration of some link failures in a WSN

External deployment conditions also add to network vulnerability. WSNs are often deployed in harsh environments where they can be exposed to adversary attacks. Such attacks can cause permanent damage to the hardware. Thus, the network will remain unable to fulfill the intended tasks (Walters et al., 2007). Since the network is managed remotely, the sensor nodes are left unattended for a long period. It is yet impossible to detect physical tampering and to perform regular maintenance.

In Figure 1, two possible causes of packet loss are illustrated. In the first case, a previously established link between the sensors is lost. Once the parent node exhausts its energy, it is dropped from the network. As a result, a child node can no longer forward the sensed data and the previously received packets are permanently lost. In the second case, more than one sensor node simultaneously try to send data packets to the same parent, resulting in a network congestion and a possible loss of all the packets being forwarded at that level.

Considering all the limitations mentioned above, it is not easy for the network to always fulfill the intended tasks. Reliability and efficiency of WSNs are dependent on key issues, which are enumerated in the following.

2.2. Dependability issues

Sensor nodes have a short radio range and they collaborate to cover a given surveillance area. At the setup phase, it is crucial to ensure that the network covers the whole area (Tian & Georganas, 2005). The coverage problem arises as: "how to ensure that, at any time, any zone in the network is covered by at least one sensor node?"

Zorbas *et al.* (Zorbas, Glynos, & Douligeris, 2007) presented B{GOP}, a centralized coverage algorithm for WSNs. The algorithm proposes sensor candidate and avoids double-coverage depending on the coverage status of the corresponding field.

In (X. Wang et al., 2003), Wang *et al.* presented a protocol that can dynamically configure a network to achieve guaranteed degrees of coverage and connectivity. They gave a proof

that sensing coverage range does not need to be more than half the connectivity range in the network. Thus, their protocol helps preserve energy while maintaining coverage in the network.

As discussed before, available energy is a big limitation to WSNs. In order to prolong the network's lifetime, a possible solution is to keep a minimum number of sensor nodes in active mode. As WSNs rely on nodes density in the sensing and communicating processes, it is very likely that some nodes will not be needed. If a reliable node can forward data packets toward the sink, its neighbors can switch to idle state temporarily. Lifetime optimization using knowledge about the dynamics of stochastic events has been studied in (He, Chen, Li, Shen, & Sun, 2012). The authors presented the interactions between periodic scheduling and coordinated sleep for both synchronous and asynchronous dense static sensor network. They show that the event dynamics can be exploited for significant energy savings by putting the sensors on a periodic on/off schedule. The authors in (Kasbekar, Bejerano, & Sarkar, 2011) leverage prediction to prolong the network life time, by exploiting temporal-spatial correlations among the data sensed by different sensor nodes. Based on Gaussian Process, the authors formulate the issue as a minimum weight submodular set cover problem and propose a centralized and a distributed truncated greedy algorithms (TGA and DTGA). They prove that these algorithms obtain the same set cover.

As sensor nodes periodically go to sleep, they need to be awake when they are requested to. This is done by the transmission of wake-up messages towards a target sensor. However, if the message is not received at the right moment, data packets will be dropped. This will cost the network extra energy due to packet retransmission (Ye, Zhong, Cheng, Lu, & Zhang, 2003; Gallais, Carle, Simplot-Ryl, & Stojmenovic, 2006; J. Bahi, Haddad, Hakem, & Kheddouci, 2011).

In WSN, if the wear-out failures are not taken into consideration during the execution of the involved application, some nodes may age much faster than the others and become the reliability bottleneck for the network, thus significantly reducing the system's service life. In the literature, this problem has been formulated and studied in various ways. For instance, prior work (He, Chen, Li, et al., 2012; He, Chen, Yau, Shao, & Sun, 2012; Kasbekar et al., 2011) in lifetime reliability assumes node's failure rates to be independent of their usage times. While this assumption can be accepted for memoryless soft failures, it is obviously inaccurate for the wear-out-related fail-silent (a faulty node does not produce any output) and fail-stop (no node recovery) failures, because the sensor node's lifetime reliability will gradually decrease over time. To cope with this problem, a distributed self-stabilizing and wear-out-aware algorithm is presented in (J. M. Bahi, Haddad, Hakem, & Kheddouci, 2013). This algorithm seeks to build resiliency by maintaining a necessary set of working nodes and replacing failed ones when needed. The proposed protocol is able to increase the lifetime of wireless sensor networks, especially when the reliability of sensor nodes is expected to decrease due to use and wear-out effects.

2.3. Attacks in WSNs

WSNs suffer from limited computation capabilities, a small memory capacity, poor energy resources, absence of infrastructure, and susceptibility to physical capture. A variety of security solutions exists for infrastructureless networks (Ad hoc networks). Yet, they do not all answer the security challenges of WSNs.

WSNs are vulnerable to many attacks, due to their uncontrolled environment of deployment, the limitation of their resources, and the broadcast nature of transmission medium. The attacks are mainly classified under two categories: physical attacks and non-physical attacks.

Examples of well-known non-physical attacks in WSNs are: Denial of Service (DoS) attack, (Walters et al., 2007; Wood & Stankovic, 2002; Kim, Doh, & Chae, 2006), sybil attack, (Walters et al., 2007; Douceur, 2002; Zhang, Wang, Reeves, & Ning, 2005), traffic analysis attack, (Walters et al., 2007; Deng, Han, & Mishra, 2004), and node replication attack (Walters et al., 2007; Parno, Perrig, & Gligor, 2005; Braginsky & Estrin, 2002).

2.4. Dependability of WSNs

The dependability of a WSN is a property that integrates the attributes needed for the application to be justifiably trusted. Such a network should be able to deliver a correct service -a service that implements the system function- and makes sure that a failed component will not lead to system failure. System dependability was defined by Avizienis in (Avizienis, Lapire, & Randell, 2000) as "the ability of a system to avoid failures that are more frequent or more severe, and outage durations that are longer, than is acceptable to the users".

Developing a dependable WSN starts with defining the dependability requirements of users. In order to satisfy these needs, it is crucial to understand what might stop the network from delivering a correct service. In the following, we enumerate the attributes of a dependable network.

2.4.1. Availability

In the classical definition, a network is considered as highly available if its downtime is very limited. This can be due either to few failures, or to quick restarts when failures take place (Knight, 2004; Taherkordi, Taleghan, & Sharifi, 2006). If we add the security aspect, we can define availability as readiness for correct service for authorized users. This attribute can be computed as the probability that the network is functioning at a given time (Silva, Guedes, Portugal, & Vasques, 2012).

2.4.2. Reliability

A reliable network is a network that is able to continuously deliver a correct service. It can also be defined as the probability that a network functions properly and continuously in a time interval (Silva et al., 2012; Taherkordi et al., 2006).
Most of research works that have been accomplished so far employ retransmission mechanisms over redundancy schemes to achieve network reliability (Silva et al., 2012). The main purpose of a WSN is the correct delivery of data packets from sensor nodes to end user. Thus, reliability of WSNs is highly related to data transport. Reliability can be classified into different levels: packet reliability, event reliability, Hop-by-Hop reliability, and End-to-End reliability.
Both packet and event reliability levels deal with the required amount of information to notify the sink of the occurrence of an event within the network environment. Whereas the remaining two levels (i.e., Hop-by-Hop and End-to-End reliability levels) are concerned with the successful recovery of event information. Yet, all of them rely on retransmission and redundancy mechanisms.

2.4.3. Security

WSNs are different from traditional computer networks. Therefore, existing security mechanisms are not suitable for these networks. Developing adequate security measures requires understanding WSNs constraints related to security issues.
An attack on a network can be extended to more than just modifying the data packets originally circulating in the network. An attacker can inject additional data packets to disturb the normal function of the network and tamper with the decision making process. For this reason, a receiver (i.e., node) must be sure that the data being accepted is coming from a member of the network. Similarly, a sender needs to verify that the reception entity is whom it claims to be. This finality can be achieved through authentication.
Benenson *et al.* based their entity authentication on elliptic curve cryptography (Benenson, Gedicke, & Ravivo, 2005). Each user holds a legitimate certificate, which is the public key signed by a certification authority. Every node can verify the legitimacy of the users since the public key with the signature are preloaded in the sensors. Yet, this scheme requires an significant overhead for data encryption.
One of the most important issues related to network security is data confidentiality, and it refers to limiting data access to legitimate destinations. Keeping data packets confidential mainly means that:

- Sensor readings can only be performed by the legitimate destination; a sensor node holding information must not leak information to its neighbors.
- Communication channel has to be secured, especially when the data being communicated is highly sensitive.
- The network needs to achieve confidentiality by encrypting data during transmissions.

In (J. M. Bahi, Guyeux, & Makhoul, n.d.), Bahi *et al.* argue that in-network communication, node scheduling, and data aggregation need to be proven as secure. For this matter, they proposed a security framework for wireless sensor networks. The authors proved that in-network communication answers to security objectives (indistinguishability, non-malleability, detection resistance). In addition to this, the proposed algorithm is able to aggregate data over encrypted packets.

2.4.4. Defensive measures

Key establishment techniques have received great attention for many years. Nevertheless, WSN applications are relatively recent. Besides, the features of these networks are different from traditional networks. Therefore, preexisting techniques for key establishment are an unsuitable solution for WSNs applications. Traditionally, key exchange techniques use asymmetric cryptography (public key cryptography). Unfortunately, low power WSNs are unable to handle such a computationally intensive technique.
The easiest way for encryption keys distribution, is to establish one single key for the entire network and forward it. It is easy to notice that this method is inefficient as one node can compromise the entire network.
An alternative solution that can be adopted is symmetric encryption key. This technique secures communication between two hosts as they share a private key that is not recognized by the rest of the network. This key will be used for both data encryption and decryption.
Another possibility is random probabilistic key distribution scheme. The initialization stage starts with preloading in every sensor node a maximum number of keys (with respect to the memory). This is done in a way that two sets of keys (in two different nodes) will at least share one key. By broadcasting the identity of the keys, every node can discover the neighbors with which it can exchange information. Now, every node can only communicate with its legitimate neighbors; a link only exists between nodes sharing a key. It is now possible for a sensor node to safely establish a link with a target node by secretly sharing a key via their neighbors (Z. Li & Gong, 2011).

3. PROGNOSTICS AND HEALTH MANAGEMENT: STATE OF THE ART

Maintenance is an important activity in industry. It is performed either to revive a machine/component, or to prevent it from breaking down. Different strategies have evolved through time, bringing maintenance to its current state. This evolution was due to the increasing demand of reliability in industry. Nowadays, plants are required to avoid shutdowns while offering both safety and reliability (Peng, Dong, & Zuo, 2010). The first form of maintenance is corrective maintenance. In

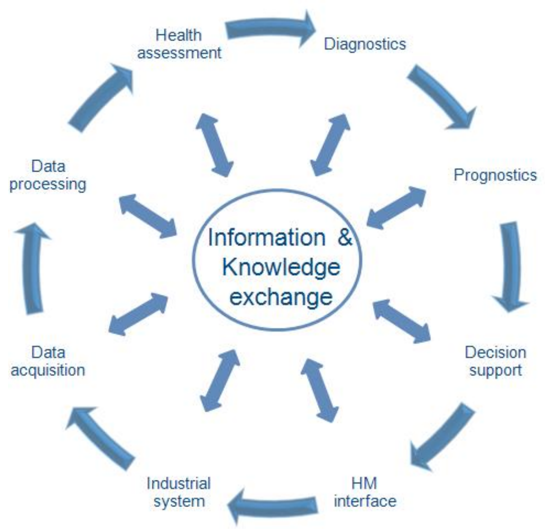

Figure 2. CBM Flowchart

this strategy, actions are only taken when the system breaks and can no longer perform the intended tasks. Yet, plants cannot afford to undergo breakdowns; in fact, sudden shutdowns cost money and time, in addition to safety and clients' trust. As a remedy to this problem, maintenance became a periodic activity. Domain experts rely on their knowledge and the observation of upcoming events to set time intervals in which the components are inspected and replaced if needed. This preventive (often called periodic) maintenance is especially adopted by transportations and nuclear plants (Hu, Youn, Wang, & Yoon, 2012). The main drawback of preventive maintenance is the fact that it is performed regardless of the machine's condition. In other words, industrials have to hire domain experts in order to set intervals for maintenance. Sometimes, this is unnecessary as the machine can be in a healthy state and this will cost extra and avoidable fees. Besides, even with periodic maintenance and inspections, random failures still occur. This is why Condition Based Maintenance (CBM) was proposed and developed in early nineties (Heng, Zhang, Tan, & Mathew, 2009).

CBM is a proactive precess for maintenance scheduling, based on real-time observations. It is an online model that assesses machine's health through condition measurements. As any maintenance strategy, CBM aims at increasing the system reliability and availability. The benefits of this particular strategy include avoiding unnecessary maintenance tasks and costs, as well as not interrupting normal machine operations (Heng et al., 2009).

In order to be efficient, a CBM program needs to go through the steps illustrated in Figure 2 (Jardine, Lin, & Banjevic, 2006).

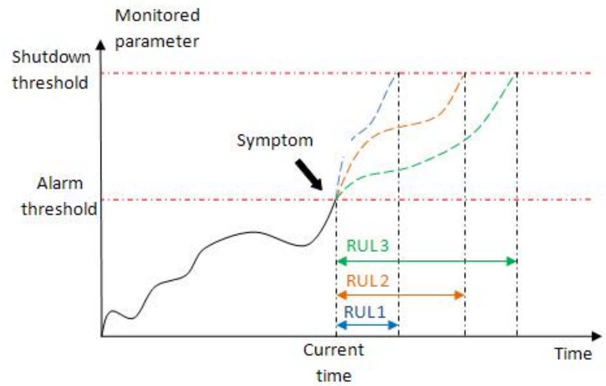

Figure 3. An illustration of RUL with uncertainties

3.1. PHM: definitions

The terms diagnostics and prognostics are widely used. Though, the difference between these two concepts is sometimes vague. However, it is important to specify the difference as it is the key to perform a good PHM.

PHM is the core activity of CBM, and it implies the same steps, namely: data processing, health assessment, diagnostics, prognostics, and decision making support.

While diagnostics aims at identifying and quantifying an actual failure, prognostics have the goal of anticipating failures. Several definitions concerning prognostics exist in the literature (ISO13381-1, 2004; D. Tobon-Mejia, Medjaher, & Zerhouni, 2012; D. A. Tobon-Mejia, Medjaher, Zerhouni, & Tripot, 2012; Zio & Maio, 2010; Jardine et al., 2006). Prognostics considers past events, the machine's current state, and operating conditions to estimate the Remaining Useful Life (RUL). This estimation is done by inspecting the evolution of continuous measurements of parameters that need to be monitored in time to assess the machine's state. These parameters can be temperature, humidity, vibration, pressure, and so on. A monitored parameter has a fixed threshold. Once reached, an alarm goes off indicating that a symptom of system deteriorating has been detected. The RUL is then computed with an associated confidence limit. The latter information illustrates to what point the predictions are trustworthy. The uncertainties of the RUL predictions have two causes: either the threshold value of monitored parameter, or the RUL prediction itself.

In Figure 3, we can observe the uncertainties that can be related to RUL prediction.

In (ISO13381-1, 2004), the necessary pre-requisites for reliable prognostics are proposed.

3.2. Classifying approaches

Prognostics approaches are classified under groups employing, more or less, the same techniques. Nevertheless, researchers use different classifications (Jardine et al., 2006),

(Heng et al., 2009), (Peng et al., 2010), (Sikorska, Hodkiewicz, & Ma, 2011), (Cadini, Zio, & Avram, 2009), (Hu et al., 2012), (D. Tobon-Mejia et al., 2012). More details on each approach can be found in the given references.
In this paper, we consider four groups: Physical models, Knowledge-based models, Data-driven models, and Hybrid models. They are detailed in the following sections.

3.2.1. Physical models:

Physical models rely on mathematical models to describe the physics of a failure, and are developed by domain experts. The first condition for a reliable model is a good understanding of the behavior of the system responding to stress. The description of the behavioral models is carried out via differential equations, state-space methods, or simulations.
Physical models are considered if:

- the mathematical model of the system is known;
- the failure mode is well understood;
- a physical model for each failure mode is available;
- the operating conditions can be monitored; and
- data describing the conditions related to each process isavailable.

Examples of model-based prognostics are given in (Y. Li, Billington, Kurfess, Danyluk, & Liang, 1999), (Byington, Watson, Edwards, & Stoelting, 2004), (Cempel, Natke, & Tabaszewski, 1997), (Qiu, Zhang, Seth, & Liang, 2002).

3.2.2. Knowledge-based models:

Since it is hard to build an accurate physical model for complex industrial systems, the employment of the latter is limited. Besides, it is impossible to apply a developed model to a different component. Other methods, such as knowledge-based ones, appear to be promising as they require no physical model.
In the following, two examples of this model are presented.

- Expert systems
  Since late 1960s, expert systems seemed to be suitable for problems usually solved by domain specialists. These models consist of computer system, designed to display expert knowledge. This knowledge is extracted by domain specialists and organized into rules learned by the computer to generate solutions.

  The rules have the form of:

  IF condition, **THEN** consequence

  Such a rule is strict and does not adapt to any changes in operating conditions. The only way to adapt the model to new situations is to add new rules whenever a new condition is observed. This can lead to a combinatorial explosion, given that a rule is required for every possible combination of inputs. Another limitation of this model is that it is only as good as its developers.

- Fuzzy logic
  It is a form of probabilistic knowledge, where the rules are approximate rather than fixed and exact. It was introduced by Zadeh in 1965 (Zadeh, 1965). The difference between fuzzy logic and classical predicate logic, is the use of fuzzy sets rather than discrete values standing for true or false. In a fuzzy set, variables membership is defined based on their degree of truth. The truth value ranges from 0 (completely wrong) to 1 (completely true).The rules may look like:

  IF condition "A" AND condition "B" **THEN** consequence.

The description associated to the parameters differs from the description used with expert system rules. Here is an example to illustrate the difference:
Expert system:

IF engine is hot **THEN** shutdown

Fuzzy logic:

IF engine is slightly hot **AND** temperature is rising **THEN** cool down the system

This new way of introducing rules gives the computer a very human-like and intuitive way of reasoning with incomplete, noisy, and inaccurate information. As a result, fault detection and prediction are more accurate, and for this reason, fuzzy logic is usually incorporated with other techniques.
Even though this method can only be developed by domain experts, it is easy to understand the developed rules. It is not only recommended because it covers a large set of operating conditions, but also because of its efficiency when it is impossible to build a mathematical model or when data contains high levels of uncertainties and noise.

3.2.3. Data-driven models:

In data-driven approaches, models are directly derived from condition monitoring data, based on statistical and machine learning techniques. These models have a double role: assess current operating conditions and predict the RUL. Neither human expertise nor comprehensive system physics are needed for the prognostic model building process.
A data-driven prognostic model transforms raw data provided by the monitoring system into useful information, which combined with historical records, helps building a behavioral model and performing predictions. The data-driven approach is popular and widely-used because it offers a reasonable tradeoff

between complexity and precision. This approach remains the best solution when obtaining reliable sensor data is much easier than constructing mathematical behavioral models. Nevertheless, accuracy depends on many factors.

- The training set: normally, an efficient training requires a large set of inputs. It is not easy to decide whether the amount of inputs we dispose of is enough for training a reliable model or not.
- Operating conditions: manufacturing conditions change all the time, so do the environmental and operational conditions. All these changes may lead to uncertainties in the predictions as they refer to new situations that may not be recognizable by the model.
- Sensory signals: the amount of effective sensory data available when prediction is performed has an impact on accuracy.
- Degradation trend: RUL prediction relies on historical data and past events. As shown in Figure 3, the prediction is an extrapolation of what we observe up to the present moment. If the degradation trend is highly similar to a trend the model can recognize, prediction can be accurate (and inversely so).

Examples of the developed methods reported in the literature are:

- Aggregate reliability functions (Crevecoeur, 1993), (Duane, 1964), (Goode, Moore, & Roylance, 2000)
- Artificial neural networks ANN (Huang et al., 2007), (Herzog, Marwala, & Heyns, 2009), (W. Wang, Golnaraghi, & Ismail, 2004)
- Autoregressive moving average ARMA (Wu, Hu, & Zhang, 2007), (Yan, Koc, & Lee, 2004)
- Bayesian techniques (Cadini et al., 2009), (Kallen & van Noortwijk, 2005), (Weidl, Madsen, & Israelson, 2005)
- Hidden markov and hidden semi-markov models (Bunks, McCarthy, & Al-Ani, 2000), (Baruah & Chinnam, 2005), (Medjaher, Tobon-Mejia, & Zerhouni, 2012)
- Proportional hazards models (Z. Li, Zhou, Choubey, & Sievenpiper, 2007), (Liao, Zhao, & Guo, 2006), (Makis & Jiang, 2003)
- Trend extrapolation (Batko, 1984), (Kazmierczak, 1983), (C.Cempel, 1987)

3.2.4. Hybrid models:

Usually, prognostic activity does not consider one parameter. The monitored parameters are diversified, making it hard to study failure behavior using only one model.

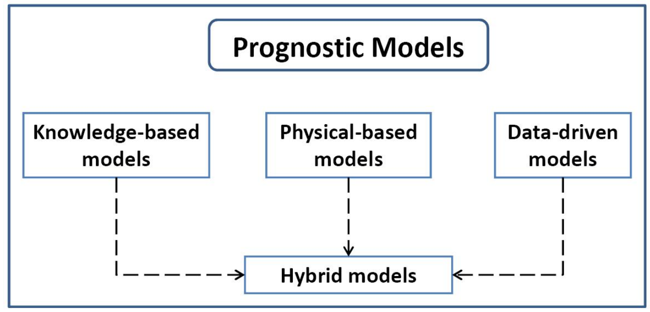

Figure 4. Categories for prognostic models

Hybrid models aim at improving prediction quality by providing more accurate RUL. All research works agree that physical models guarantee the most precise prediction. Nevertheless, even with good output quality, the complexity is too significant to ignore. This complexity can be reduced by adopting a data-driven approach. Thus, we can benefit from the merits of both prognostic approaches.
When physical understanding of failure mechanism and monitoring data are available, a hybrid approach is the best solution offering a compromise between model complexity and prediction accuracy.
In Figure 4 we illustrate the categories for prognostic models.

4. WSNS FOR INDUSTRIAL PHM AND CHALLENGES AHEAD

Reliability has become very essential in industry. It is a means to financial gain in addition to client trust. The research in the prognostic field, over the past years, resulted in a variety of tools and techniques offering plants the possibility to survey their systems, anticipate failures, and schedule maintenance. As the existent tools are different from one another, they have different advantages, drawbacks, complexities, etc. Data driven prognostic models drew a great deal of attention due to their low cost, low complexity, and easy deployment. The prediction model will first acquire information about the monitored system, assess the current state, and then extrapolate its future health state.
WSNs are mainly designed for surveillance purposes. They can be deployed in many fields such as military, automotive, agriculture, medicine...(Z. Li & Gong, 2011). Recently, industry has given WSN monitoring applications a great deal of attention. Nowadays, sensor networks are used to monitor industrial machinery for maintenance scheduling. The sensors deployed to survey the system/component will provide data to estimate the RUL. Nevertheless, if this data is inaccurate, the prediction based on it will not be relevant. The dependability requirements, discussed before, need to be considered before the network starts running. Thereby, they can provide accurate data for RUL prediction and maintenance scheduling. Despite the existence of many dependability solutions in WSNs, these solutions are not always applicable. As sensors

have restricted computational capabilities, solutions are often application oriented. Thus, a definition of dependability issues related to prognostics is essential.
Many aspects still need further studying in order to provide more reliable predictions. How can we explore available data? How can we consider operating conditions in RUL prediction? How can we allow multiple interactions while building a model? All these questions still need answers.
Data-driven models are designed to reduce model complexity and enhance real-time maintenance. For this matter, they only provide general predictions for a population of identical units; this makes prediction process easier and faster.
In the literature of prognostics, it is very common that the causes of a failure are limited to the values of monitored parameters. Other factors, although responsible for failures, seem to be neglected and overlooked. Although Condition Monitoring (CM) data reflects online monitoring, it does not replace reliability data. In fact, CM data provides measurements informing about a single component state at a specific moment. A failure does not only consider a single parameter (pressure, humidity...), it is a consequence of many factors (component age, different failing components...).
Reliability data, informing about all these factors, gives a bigger picture of the failing process. We are not neglecting the importance of CM data for prognostic process. However, while CM data provides information for short-term prediction, reliability data is able to extend these predictions until the next maintenance window. The complete neglection of operating conditions, operating age, and interactions between failures can only limit the application of developed models to real machines. Operating conditions are constantly changing, and if the model is unable to consider these changes, it is unable to produce reliable estimations. Furthermore, if we observe two similar components with different operating ages and operating under similar conditions, we will notice that they will not fail at the same time. Operating age definitely has an influence on time to failure. An internal failure can even accelerate or provoke another one.
Another issue to face while performing prognostics, is censored data. Many plants do not allow their system to run to failure. Components are often replaced before they actually fail. As a result, the real time to failure is not recorded. The performed preventive maintenance is mistaken for failure time, and RUL prediction is based upon that time. The value of RUL is critical for maintenance scheduling. In other words, the less accurate the prediction, the less reliable the maintenance schedule will be.
Maintenance scheduling is the reason behind building prognostic models. Once accomplished, the maintenance actions are not always considered in the model and generally, the related component is considered "as good as new". It is very important to consider the effects of maintenance actions in the prediction model, at least to evaluate the model efficiency and study the new failure behavior after the maintenance being performed.
What also drew our attention are the assumptions made to perform predictions. To the best of our knowledge, none of the previous research works has questioned the availability, safety, and security of data used for RUL prediction. It is assumed that:

- Sensory data is available and there is no data loss.
- The sensor network is reliable.
- There is no fault in the sensors.
- There is no constraint on energy consumption

So far, all prognostic work is limited to the condition monitoring layer, the health assessment layer, and the prognostic layer of the Open System Architecture for Condition-Based Maintenance OSA-CBM (Thurston, 2001; Niu & Yang, 2010). As RUL prediction concerns results that are yet to come, it has to rely on assumptions. Nevertheless, these assumptions, in no way, reflect a real life situation. The application of Wireless Sensor Networks (WSN) is very critical. First of all, the sensors size is very small. So they have very small batteries with limited disposable energy. If the communication in the network does not consider this limitation, the sensors will quickly consume all the energy they have and be dropped. Thus, the information will no longer circulate in the network. Still, an energy efficient WSN will not stop some nodes from being dropped. This means that the network has to be fault tolerant in order to be able to pursue its functionalities in case of any sudden events (sensor loss, interferences...). Besides, like all wireless networks, WSN can be hacked. Competitors and hackers can steal information, change data, cause damage to the system... Data circulating in the network needs to be secured against such attacks.
Many research works have been done in the field of WSN reliability. But every application has its own features, and generalized solutions do not always solve the problem. An adapted solution for prognostics needs and goals should be considered.

5. CONCLUSION

Condition-based maintenance is an important tool for modern plants in order to optimize their maintenance schedule. An appropriate schedule is reflected by the economical benefits. This paper went through the CBM process and its different steps leading to prognostics, and presented the different methods used in the literature of the latter to estimate the remaining useful life. Choosing one model over another mainly depends on (1) the available information to perform predictions and to study the systems behavior, (2) the complexity of the model, and (3) preferences regarding the domain of application, advantages and drawbacks of each model.
This paper also highlighted the fact that prognostic field still needs several improvements. RUL predictions cannot be ac-

curate if several points are not considered while building a model, namely (1) WSN dependability, (2) securing data, (3) including event data and censored data in the prediction process, and (4) model updates.

A discussion of dependability in WSNs is also given in this paper. In order to build a dependable network several attributes need to be considered: (1) network availability, (2) network reliability, and (3) network security. These attributes are the key for accurate data and reliable predictions.

REFERENCES

Akan, O. B., & Akyildiz, I. F. (2005, October). Event-to-sink reliable transport in wireless sensor networks. *IEEE/ACM Transactions on Networking*, *13*(5), 1003-1016.

Avizienis, A., Lapire, J.-C., & Randell, B. (2000). *Fundamental concepts of dependability* (Tech. Rep.). University of Newcastle.

Bahi, J., Haddad, M., Hakem, M., & Kheddouci, H. (2011). Distributed lifetime optimization in wireless sensor netwoks. In *Hpcc* (p. 432-439).

Bahi, J. M., Guyeux, C., & Makhoul, A. (n.d.). A security framework for wireless sensor networks: Theory and practice.

Bahi, J. M., Haddad, M., Hakem, M., & Kheddouci, H. (2013). Stabilization and lifetime optimization in distributed sensor networks. In *Aina* (pp. 437–442).

Baruah, P., & Chinnam, R. (2005, March). Hmms for diagnostics and prognostics in machining process. *International journal of Production Research*, *43*(6), 1275-1293.

Batko, W. (1984). *Prediction method in technical diagnostics*. Unpublished doctoral dissertation, Cracov Mining Academy.

Benenson, Z., Gedicke, N., & Ravivo, O. (2005). Realizing robust user authentification in sensor netwoks. In *Real-world wireless sensor networks (realwsn'05).*

Braginsky, D., & Estrin, D. (2002). Rumor routing algorithm for sensor netwoks. In *1st acm international workshop on wireless sensor networks and applications* (p. 22-31). NY, USA: ACM Press.

Bunks, C., McCarthy, D., & Al-Ani, T. (2000). Condition-based maintenance of machines using hidden markov models. *Mechanical Systems and Signal Processing*, *14*(4), 597-612.

Byington, C., Watson, M., Edwards, D., & Stoelting, P. (2004, March). A model-based approach to prognostics and health management for flight control actuators. In *Proceedings of the ieee aerospace conference* (Vol. 6, p. 3351-3362).

Cadini, F., Zio, E., & Avram, D. (2009). Model-based monte carlo state estimation for condition-based component replacement. *Reliability Engieneering and System Safety*, *94*, 752-758.

Carman, D. W., Kuus, P. S., & Matt, B. J. (2000, September). *Constraints and approaches for distributed sensor network security* (Tech. Rep.). NAI Labs, The Security Research Division, Network Associates, Inc. Glenwood.

C.Cempel. (1987). Simple condition forecasting techniques in vibroacoustical diagnostics. *Mechanical Systems and Signal Processing*, *1*, 75-82.

Cempel, C., Natke, H., & Tabaszewski, M. (1997). A passive diagnostic experiment with ergodic properties. *Mechanical Systems and Signal Processing*, *11*, 107-117.

Crevecoeur, G. (1993). A model for the integrity assessment of ageing repairable systems. *IEEE Transactions on Reliability*, *42*(1), 148-155.

Deng, J., Han, R., & Mishra, S. (2004). *Countermeasures against traffic analysis attacks in wireless sensor netwoks* (Tech. Rep.). University of Colorado.

Douceur, J. R. (2002, February). The sybil attack. In *Proceedings of the first international workshop on peer-to-peer systems (iptps'02).*

Duane, J. (1964). Learning curve approach to reliability monitoring. *IEEE Transactions on Aerospace*, *2*(2), 563-566.

Gallais, A., Carle, J., Simplot-Ryl, D., & Stojmenovic, I. (2006). Localized sensor area coverage with low communication overhead. In *Proceedings of the fourth annual ieee international conference on pervasive computing and communications* (pp. 328–337).

Goode, K., Moore, J., & Roylance, B. (2000). Plant machinery working life prediction method utilizing reliability and condition-monitoring data. *Proceedings of the IMechE, PartE: Journal of Process Mechanical Engineering*, *214*(E2), 109-122.

He, S., Chen, J., Li, X., Shen, X. S., & Sun, Y. (2012). Leveraging prediction to improve the coverage of wireless sensor networks. *IEEE Trans. Parallel Distrib. Syst.*, *23*(4), 701-712.

He, S., Chen, J., Yau, D. K. Y., Shao, H., & Sun, Y. (2012). Energy-efficient capture of stochastic events under periodic network coverage and coordinated sleep. *IEEE Trans. Parallel Distrib. Syst.*, *23*(6), 1090-1102.

Heng, A., Zhang, S., Tan, A. C., & Mathew, J. (2009). Rotating machinery prognostics: State of the art, challenges and opportunities. *Mechanical Systems and Signal Processing*, *23*, 724-739.

Herzog, M., Marwala, T., & Heyns, P. (2009). Machine and component residual life estimation through the application of neural netwoks. *Reliability Engieneering and System Safety*, *94*(2), 479-489.

Hu, C., Youn, B. D., Wang, P., & Yoon, J. T. (2012). Ensemble of data-driven prognostic algorithms for robust prediction of remaining useful life. *Reliability Engieneering and System Safety*, *103*, 120-135.

Huang, R., Xi, L., Li, X., Liu, C. R., Qiu, H., & Lee, J. (2007). Residual life prediction for ball bearings based on self-organizing map and back propagation neural network methods. *Mechanical Systems and Signal Processing*, *21*(1), 193-207.

ISO13381-1. (2004). *Condition monitoring and diagnostics of machines- prognostics- part1: General guidelines.*

Jardine, A. K., Lin, D., & Banjevic, D. (2006). A review on machinery diagnostics and prognostics implementing condition-based maintenance. *Mechanical Systems and Signal Processing*, *20*, 1483-1510.

Kallen, M., & van Noortwijk, J. (2005). Optimal maintenance decisions under imperfect inspection. *Reliability Engieneering and System Safety*, *90*, 177-185.

Kasbekar, G. S., Bejerano, Y., & Sarkar, S. (2011). Lifetime and coverage guarantees through distributed coordinate-free sensor activation. *IEEE/ACM Trans. Netw.*, *19*(2), 470-483.

Kazmierczak, K. (1983). Application of autoregressive prognostic techniques in diagnostics. In *The vehicle diagnostics conference.* Tuczno, Poland.

Kim, M., Doh, I., & Chae, K. (2006, February 20-22). Denial of service (dos) detection through practical entropy estimation on hierarchical sensor networks. In *The 8th international conference advanced communication technology icact* (Vol. 3, p. 1566-1571).

Knight, J. C. (2004). An introduction to computing system dependability. In *Proceedings of the 26th international conference on software engineering (icse'04).*

Li, Y., Billington, S., Kurfess, T., Danyluk, S., & Liang, S. (1999). Adaptive prognostics for rolling element bearing condition. *Mechanical Systems and Signal Processing*, *13*, 103-113.

Li, Z., & Gong, G. (2011). *A survey on security in wireless sensor netwoks* (Vols. –; Tech. Rep.). Canada: Department of Electrical and Computer Engineering, University of Waterloo.

Li, Z., Zhou, S., Choubey, S., & Sievenpiper, C. (2007). Failure event prediction using the cox proportional hazard model driven by frequent failure signatures. *IIE Transactions*, *39*, 303-315.

Liao, H., Zhao, W., & Guo, H. (2006, January). Predicting remaining useful life of an individual unit using proportional hazards model and logistic regression model. In *Reliability and maintainability symposium* (p. 127-132).

Makis, V., & Jiang, X. (2003). Optimal replacement under partial observations. *Mathematics of Operations Research*, *28*(2), 382.

Medjaher, K., Tobon-Mejia, D., & Zerhouni, N. (2012, June). Remaining useful life estimation of critical components with application to bearings. *IEEE Transactions on Reliability*, *61*(2), 292-302.

Niu, G., & Yang, B.-S. (2010). Intelligent condition monitoring and prognostics system based on data-fusion strategy. *Expert Systems with Applications*, *37*, 8831-8840.

Parno, B., Perrig, A., & Gligor, V. (2005, May). Distributed detection of node replication attacks in sensor networks. In *Ieee sympsium on security and privacy.*

Peng, Y., Dong, M., & Zuo, M. J. (2010). Current status of machine prognostics in condition-based maintenance: a review. *International journal of Advanced Manifacturing Technology*, *50*, 297-313.

Qiu, J., Zhang, C., Seth, B., & Liang, S. (2002). Damage mechanics approach for bearing lifetime prognostics. *Mechanical Systems and Signal Processing*, *16*, 817-829.

Sikorska, J., Hodkiewicz, M., & Ma, L. (2011). Prognostic modelling options for remaining useful life estimation by industry. *Mechanical Systems and Signal Processing*, *25*, 1803-1836.

Silva, I., Guedes, L. A., Portugal, P., & Vasques, F. (2012). Reliability and availability evaluation of wireless sensor netwoks for industrial applications. *Sensors*, *12*, 806-838.

Taherkordi, A., Taleghan, M. A., & Sharifi, M. (2006, December). Dependability considerations in wireless sensor netwoks applications. *Journal of Networks*, *1*(6), 28-35.

Thurston, M. (2001). An open standard for web-based condition-based maintenance systems. In I. S. R. T. Conference (Ed.), *Autotestcon proceedings* (p. 401-415).

Tian, D., & Georganas, N. D. (2005). Connectivity maintenance and coverage preservation in wireless sensor networks. *Ad Hoc Networks*, *3*, 744-761.

Tobon-Mejia, D., Medjaher, K., & Zerhouni, N. (2012). Cnc machine tool's wear diagnostic and prognostic by using dynamic bayesian networks. *Mechanical Systems and Signal Processing*, *28*, 167-182.

Tobon-Mejia, D. A., Medjaher, K., Zerhouni, N., & Tripot, G. (2012, June). A data-driven failure prognostics method based on mixture of gaussians hidden markov models. *IEEE Transactions on Reliability*, *61*(2), 491-503.

Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network security: A survey. In *Security in distributed, grid and pervasive computing* (p. 799-849). CRC Press.

Wang, W., Golnaraghi, M., & Ismail, F. (2004). Prognostics of machine health condition using neuro-fuzzy systems. *Mechanical Systems and Signal Processing*, *18*, 813-831.

Wang, X., Xing, G., Zhang, Y., Lu, C., Pless, R., & Gill, C. (2003). Integrated coverage and connectivity configuration in wireless sensor netwoks. In *First acm conference on embedded networked systems.*

Weidl, G., Madsen, A., & Israelson, S. (2005). Applications of object-oriented bayesian networks for condi-

tion monitoring, root cause analysis and desicion support on operation of complex continuous process. *Computers and Chemical Engineering*, *29*, 1996-2009.

Wood, A. D., & Stankovic, J. A. (2002, October). Denial of service in sensor networks. *Computer*, *35*(10), 54-62.

Wu, W., Hu, J., & Zhang, J. (2007). Prognostics of machine healt condition using an improved arma-based prediction method. In *Ieee* (p. 1062-1067). China.

Yan, J., Koc, M., & Lee, J. (2004). A prognostic algorithm for machine performance assessment and its application. *Production Planning and Control*, *76*, 796-801.

Ye, F., Zhong, G., Cheng, J., Lu, S., & Zhang, L. (2003). Peas: A robust energy conserving protocol for long-lived sensor networks. In *Proceedings of the 23rd international conference on distributed computing systems* (pp. 28–37).

Zadeh, L. A. (1965). Fuzzy sets. *Information and control*, *8*, 338-353.

Zhang, Q., Wang, P., Reeves, D. S., & Ning, P. (2005). Defending against sybil attacks in sensor networks. In *25th ieee international conference on distributed computing systems workshops* (p. 185-191).

Zio, E., & Maio, F. D. (2010). A data-driven fuzzy appoach for predicting the remaining useful life in dynamic failure scenarios of a nuclear system. *Reliability Engieneering and System Safety*, *95*, 49-57.

Zorbas, D., Glynos, D., & Douligeris, C. (2007). BGOP: An adaptive algorithm for coverage problems in wireless sensor netwoks. In *the 13th european wireless conference.*